Remarks

Reconsideration of this Application is respectfully requested.

Claims 1-23 are pending in the application, with claims 1 and 13 being the independent claims. Based on the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 103

Matthews and Hronik

In the Office Action, claims 1, 5-9, 11-13, 17-21, and 23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Matthews, Jr., U.S. Patent No. 6,549,622 (Matthews) in view of Hronik, U.S. Publication No. 2003/0167374 (Hronik). Applicant respectfully traverses this rejection.

In the rejection, the Examiner stated that although "Matthews does not explicitly disclose a memory for performing a plurality of write data operations in a single cycle," this element is described in Hronik. However, "the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination." *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990). No suggestion or motivation to combine the references to achieve Applicant's invention is present in Matthews and Hronik.

Matthews describes a first embodiment using a single dual port memory (i.e., a single input port to obtain write data and a single output port to provide read data). (Matthews, col. 4, lines 26-30; Fig. 5). In the modified RC4 algorithm for the first embodiment, the dual port memory, at most, is operable to perform a single read and a

single write operation in a single cycle. (Matthews, col. 4, lines 40-45) (*See* specifically the description of cycles (3) and (4)).

Matthews also describes a second embodiment using two dual port memories. In the modified RC4 algorithm for the second embodiment, a cycle requires at most two read operations and a single write operation. (Matthews, col. 4, line 60 - col. 5, line 9)(*See* specifically the description of cycle (4)). The use of two dual port memories enables the performance of "two 'load' operations, an 'add' operation and a 'store' operation in the same cycle [i.e., cycle (4)]." (Matthews, col. 7, lines 51-58).

As described in Applicant's specification, the read and write operations in the RC4 algorithm have certain dependencies. (Specification, p. 1, lines 23-34). Even assuming arguendo that the system of Matthews incorporated a memory operable to perform multiple writes in the same cycle, nowhere does Matthews teach or suggest any modification to the RC4 algorithm processing to overcome the read/write dependencies to allow for the performance of multiple writes in a single cycle. In fact, the RC4 processing described in Matthews would still require multiple cycles to produce one byte of the key stream. Thus, the combination of Matthews and Hronik does not result in the single cycle multi-port core recited in Applicant's claims 1 and 13.

Furthermore, Applicant's claimed invention is specifically designed to improve on limitations of Matthews:

> If a dual ported memory is used, the performance can be increased such that a byte of key stream can be generated every 3 cycles. According to various embodiments, the memory is implemented as a 5-ported memory and the performance of the ARC4 [i.e., RC4] engine is that one byte of key stream is generated every cycle. This is a 3 or 5 times performance improvement over the conventional approach.

(Specification, p. 14, lines 12-17). Thus, the claimed invention which recites "a plurality of input ports configured to obtain write data associated with a stream cipher" and "a plurality of output ports configured to provide read data associated with the stream cipher" is an improvement over the prior art.

Based on the foregoing, Applicant submits that no motivation to combine Matthews and Hronik to achieve Applicant's invention exists. For at least these reasons, independent claims 1 and 13 are patentable over the combination of Matthews and Hronik. Claims 5-9, 11, and 12 depend from claim 1 and claims 17-21 and 23 depend from claim 13. For at least the above reasons, and further in view of their own features, claims 5-9, 11, 12, 17-21, and 23 are patentable over the combination of Matthews and Hronik. Reconsideration and withdrawal of this rejection is therefore respectfully requested.

Matthews, Hronik, and Kundarewich

Claims 2-3 and 14-15 were rejected under 35 U.S.C §103(a) as being unpatentable over Matthews in view of Hronik and further in view of Kundarewich, et al, "A CPLD-based RC4 cracking system." (Kundarewich). Applicant respectfully traverses this rejection.

Claims 2 and 3 depend from claim 1 and claims 14 and 15 depend from claim 13. Kundarewich does not overcome all of the deficiencies of Matthews and Hronik relative to claims 1 and 13 described above. For at least these reasons, and further in view of their own features, claims 2, 3, 14, and 15 are patentable over the combination of Matthews and Hronik in view of Kundarewich. Reconsideration and withdrawal of the ground of rejection is therefore respectfully requested.

Matthews, Hronik, Kundarewich, Correale, Jr.

Claims 4 and 16 were rejected under 35 U.S.C §103(a) as being unpatentable over Matthews in view of Hronik and in view of Kundarewich, further in view of Correale, Jr., U.S. Patent 4,998,221 (Correale). Applicant respectfully traverses this rejection.

Claims 4 depends from claim 1 and claim 16 depends from claim 13. Correale does not overcome all of the deficiencies of Matthews, Hronik, and Kundarewich relative to claims 1 and 13 described above. For at least these reasons, and further in view of their own features, claims 4 and 16 are patentable over the combination of Matthews, Hronik, Kundarewich, and Correale. Reconsideration and withdrawal of the ground of rejection is therefore respectfully requested.

Matthews, Hronik, and Schneier

Claims 10 and 22 were rejected under 35 U.S.C §103(a) as being unpatentable over Matthews in view of Hronik and further in view of Schneier, "Applied Cryptography." (Schneier). Applicant respectfully traverses this rejection.

Claim 10 depends from claim 1 and claim 22 depends from claim 13. Schneier does not overcome all of the deficiencies of Matthews and Hronik relative to claims 1 and 13 described above. For at least these reasons, and further in view of their own features, claims 10 and 22 are patentable over the combination of Matthews, Hronik, and Schneier. Reconsideration and withdrawal of the ground of rejection is therefore respectfully requested.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicant
Registration No. 50,633

Date: June 28, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

551056_1.DOC